IN THE CLAIMS

Please amend the claims as follows:

Claim 1 (Currently Amended): A method of encrypting an input data string including a plurality of bits of binary data with a processing device communicatively coupled to a memory having executable instructions stored therein which cause the processing device to implement a method of encryption, the method comprising:

receiving the input data string for encryption at the processing device;

providing a control code index in the memory, the control code index being defined prior to encryption at the processing device, the control code index including a plurality of control codes each defining respective orders of n bit combinations of binary data, the respective orders of bit combinations of each control code defining control code segments;

determining an order in which to query the presence of each of 2^n different configurations of n bits within the input data string, the determined order being selected without any analysis of the input data string;

identifying a control code associated with the determined order using the control code index;

generating a position code using the identified control code in cooperation with a position code routine associated with the identified control code to determine positions of each of the 2^n different configurations of n bits in the input data string by comparing the 2^n different configurations of n bits within the input data string with a first one of the control code segments of the identified control code to identify which n bit segments of the input data string correspond to a first n bit segment within the control code ~~the 2^n different configurations of the of the input data string which correspond to the first one of the control code segments~~, comparing additional ones of the control code segments in a serial fashion to previously unidentified ones of the ~~2^n different configurations of the data string~~ n bit segments of the input data string, correspondences to the control code segment comparisons resulting in output values dictated by the position code routine which defines the generated position code; and

combining the identified control code and the generated position code as components of an encrypted data string.

Claims 2 (Canceled).

Claim 3 (Previously Presented): The method of Claim 1, wherein determining an order comprises selecting a predetermined order.

Claim 4 (Canceled).

Claim 5 (Previously Presented): The method of Claim 1, further comprising:

dividing the input data string into a plurality of blocks of data.

Claim 6 (Previously Presented): The method of Claim 5, wherein the number of bits within each of the plurality of blocks of data is individually determined in response to a random number generator.

Claim 7 (Previously Presented): The method of Claim 5, wherein dividing the input data string into a plurality of blocks of data, includes determining the individual number of bits within each of the plurality of blocks of data in accordance with a rule set.

Claim 8 (Previously Presented): The method of Claim 5, further comprising: generating a plurality of block codes associated with a plurality of blocks of data of the input data string, each block code indicating the number of bits within the associated block of data.

Claim 9 (Previously Presented): The method of Claim 8, further comprising: combining each of the plurality of block codes with the identified control code and the generated position code for the associated block of data.

Claims 10-20 (Canceled).

Claim 21 (Currently Amended): A method for encrypting an input data string, including a plurality of bits of binary data, the method comprising:

receiving the input data string for encryption;

providing a control code index, the control code index being defined prior to encryption, the control code index including a plurality of control codes each defining respective orders of n bit combinations, of binary data the respective orders of bit combinations of each control code defining control code segments;

determining an order in which to query the presence of each of 2^n different configurations of n bits within the input data string, the determined order being selected without any analysis of the input data string;

identifying a control code associated with the determined order using the control code index;

generating a position code using the identified control code in cooperation with a position code routine associated with the identified control code to determine positions of each of the 2^n different configurations of n bits in an input data string by comparing the 2^n

different configurations of n bits within the input data string with a first one of the control code segments of the identified control code to identify ~~the 2^n different configurations of the of the input data string which correspond to the first one of the control code segments~~ which n bit segments of the input data string correspond to a first n bit segment within the control code, comparing additional ones of the control code segments in a serial fashion to previously unidentified ones of the ~~2^n different configurations of the data string~~, n bit segments of the input data string correspondences to the control code segment comparisons resulting in output values dictated by the position code routine which defines the generated position code; and

combining the identified control code and the generated position code as components of an encrypted data string.

Claim 22 (Previously Presented): The method of Claim 21, further comprising arranging the input data string into a plurality of data blocks.

Claim 23 (Currently Amended): A computer readable storage medium including computer program instructions that cause a computer to implement a method of encrypting an input data string, including a plurality of bits of binary data, the method comprising:

receiving the input data string for encryption;

providing a control code index that is defined prior to encryption, the control code index including a plurality of control codes each defining respective orders of n bit combinations of binary data, the respective orders of bit combinations of each control code defining control code segments;

determining an order in which to query the presence of each of 2^n different configurations of n bits within the input data string, the determined order being selected without any analysis of the input data string;

identifying a control code associated with the determined order using the control code index;

generating a position code using the identified control code in cooperation with a position code routine associated with the identified control code to determine the positions of each of the 2^n different configurations of n bits in the input data string by comparing the 2^n different configurations of n bits within the input data string with a first one of the control code segments of the identified control code to identify ~~the 2^n different configurations of the of the input data string which correspond to the first one of the control code segments~~ which n bit segments of the input data string correspond to a first n bit segment within the control code, comparing additional ones of the control code segments in a serial fashion to previously unidentified ones of the ~~2^n different configurations of the data string~~ n bit segments of the input data string, correspondences to the control code segment comparisons resulting in output values dictated by the position code routine which defines the generated position code; and

combining the identified control code and the generated position code as components of an encrypted data string.

Claims 24 (Canceled).

Claim 25 (Currently Amended): The computer readable storage medium including computer program instructions of Claim 23, that cause a computer to implement a method ,wherein determining an order includes selecting a predetermined order.

Claim 26 (Currently Amended): The ~~method~~ tangible computer readable storage medium of Claim 23, that cause a computer to implement a method ,further comprising:

dividing the input data string into a plurality of blocks of data.

Claim 27 (Currently Amended): The ~~method~~ computer readable storage medium of Claim 26, that cause a computer to implement a method ,wherein dividing the input data string into a plurality of blocks of data includes determining the individual number of bits within each of the plurality of blocks of data in response to a random number generator.

Claim 28 (Currently Amended): The ~~method~~ computer readable storage medium of Claim 26 that cause a computer to implement a method, wherein dividing the input data string into a plurality of blocks of data, includes determining the individual number of bits within each of the plurality of blocks of data in accordance with a rule set.

Claim 29 (Currently Amended): The ~~method~~ computer readable storage medium of Claim 26 that cause a computer to implement a method, wherein determining an order further comprises:

determining a first order associated with a first block of data and determining a second order associated with a second block of data wherein the first order is different than the second order.

Claim 30 (Currently Amended): The ~~method~~ computer readable storage medium of Claim 26 that cause a computer to implement a method, wherein the computer program instructions further ~~comprising~~ comprise:

generating a plurality of block codes associated with a plurality of blocks of data, each block code indicating the number of bits within the associated block of data.

Claim 31 (Currently Amended): The ~~method~~ computer readable storage medium of Claim 30 that cause a computer to implement a method, wherein the computer program instructions further ~~comprising~~ comprise:

combining the each of the plurality of block codes with the identified control code and the generated position code for the associated block of data.

Claims 32-33 (Canceled).

Claim 34 (Currently Amended): The ~~method~~ computer readable storage medium of Claim 23 that cause a computer to implement a method, , wherein identifying the control code includes randomly selecting the control code via a random number generator.

Claim 35 (Currently Amended): The ~~method~~ computer readable storage medium of Claim 23 that cause a computer to implement a method, wherein determining an order includes generating an order using a rule set.

Claim 36-37 (Canceled).

Claim 38 (Currently Amended): The ~~method~~ computer readable storage medium of Claim 3 that cause a computer to implement a method, wherein determining the order in which to query the presence of each of 2^n different configurations of n bits of binary data within an input data string includes determining the order in which to query the presence of each of 4 different configurations of 2 bits within an input data string.

Claim 39-40 (Canceled)

Claim 41 (Currently Amended): The ~~method~~ computer readable storage medium of Claim 23 that cause a computer to implement a method ,wherein the computer program instruction, further ~~comprising~~ comprise performing a further encryption of the encrypted data string.

Claim 42 (Currently Amended): The ~~method~~ computer readable storage medium of Claim 41 that cause a computer to implement a method, wherein encrypting the encrypted data string comprises:

providing an encryption key having a first selected number of bits; and

performing an XOR function between the encryption key and the encrypted data string.

Claim 43 (Currently Amended): The ~~method~~ computer readable storage medium of Claim 41 that cause a computer to implement a method, wherein encrypting the encrypted data string comprises:

determining an order in which to query the presence of each of 2^n different configurations of n bits within the input data string;

identifying a second control code associated with the determined order using the control code index each control code defining respective orders of n bit combinations of binary data;

generating a position code using the identified control code in cooperation with a position code routine associated with the identified control code to determine positions of each of the 2^n different configurations of n bits in the input data string by comparing the 2^n

different configurations of the input data string with the associated 2^n bit configurations of the identified control code, the comparisons resulting in output values dictated by the position code routine which defines the generated position code; and

combining the second identified control code and the second generated position code to create a different encrypted version of the encrypted data string.

Claim 44 (Currently Amended): The <u>computer readable storage medium</u> of Claim 25 that cause a computer to implement a method, wherein selecting a predetermined order includes selecting a default order.

Claims 45-47 (Canceled).

Claim 48 (Previously Presented): The method of Claim 1, wherein identifying the control code includes randomly selecting the control code via a random number generator.

Claim 49 (Previously Presented): The method of Claim 1, wherein determining an order includes generating an order using a rule set.

Claim 50 (Previously Presented): The method of Claim 5, wherein determining an order includes determining a first order associated with a first block of data and determining a second order associated with a second block of data wherein the first order is different than the second order.

Claim 51-52 (Canceled).

Claim 53 (Previously Presented): The method of Claim 1, wherein determining the order in which to query the presence of each of 2^n different configurations of n bits within an input data string includes determining the order in which to query the presence of each of 4 different configurations of 2 bits within an input data string.

Claim 54 (Canceled).

Claim 55 (Canceled).

Claim 56 (Previously Presented): The method of Claim 1, further comprising: performing a further encryption of the encrypted data string.

Claim 57 (Previously Presented): The method of Claim 56, wherein performing a further encryption of the encrypted data string, further comprises:

providing an encryption key having a first selected number of bits; and

performing an XOR function between the encryption key and the encrypted data string.

Claim 58 (Previously Presented): The method of Claim 56, wherein performing a further encryption of the encrypted data, further comprises:

determining an order in which to query the presence of each of 2^n different configurations of n bits within the input data string each control code defining respective orders of n bit combinations of binary data;

identifying a second control code associated with the determined order using the control code index;

generating a position code using the identified control code in cooperation with a position code routine associated with the identified control code to determine positions of each of the 2^n different configurations of n bits in the input data string by comparing the 2^n different configurations of the input data string with the associated 2^n bit configurations of the identified control code, the comparisons resulting in output values dictated by the position code routine which defines the generated position code; and

combining the second identified code and the second generated position code to create a different encrypted version of the encrypted data string.

Claim 59 (Previously Presented): The method of Claim 3, wherein selecting a predetermined order includes selecting a default order.

Claims 60-61 (Canceled).

Claim 62 (Currently Amended): An electronic device for encrypting an input data string, including a plurality of bits of binary data, comprising:

a processor configured to receive the input data string for encryption;

a memory configured to include a control code index, the control code index being defined prior to encryption by the processor, the control code index including a plurality of control codes, the control codes having corresponding values each defining respective orders of n bit combinations of binary data, the respective orders of bit combinations of each control code defining control code segments, wherein the processor is operably linked to the memory for determining upon reception of the input data string, an order in which to query the presence of each of two 2^n different configurations of n bits within the input data string, the determined order being selected without any analysis of the input data string, and identifies a control code associated with the determined order by access of the control code index, the processor generating a position code, using the identified control code in cooperation with a position code routine associated with the identified with the identified control code to determine positions of each of the two 2^n different configurations of n bits in the input data string by comparing the 2^n different configurations of n bits within the input data string with a first one of the control code segments of the identified control code to identify the~~ 2^n different configurations of the of the input data string which correspond to the first one of the control code segments~~ which n bit segments of the input data string correspond to a first n bit segment within the control code, comparing additional ones of the control code segments in a serial fashion to previously unidentified ones of the ~~2^n different configurations of the data string~~ n bit segments of the input data string, correspondences to the control code segment comparisons resulting in output values dictated by the position code routine which defines the generated position code to combine the identified control code and the generated position code as components of an encrypted data string.